OCCUPATIONAL GROUP: Information Technology

CLASS FAMILY: **Security**

CLASS FAMILY DESCRIPTION:

This family of positions provides security and monitoring for the transmission of information in voice, data, and/or video formats over the internal network.

CLASS TITLE: Information Security Analyst 1

DISTINGUISHING CHARACTERISTICS:
These positions perform full-performance level technical work in developing, implementing and maintaining information security policies, standards and controls. They assist with audits and assessments to identify and analyze potential threats to data and systems. These positions recommend internal controls and risk management strategies, and assume lead responsibility for the planning, development, implementation and ongoing management of at least one information security program. These positions typically do not have budgetary responsibilities, but may serve as lead workers. Perform related work as required.

EXAMPLES OF WORK: ***(Any specific position in this class may not include all of the duties listed; nor do the examples listed cover all of the duties which may be assigned.)***

- Supports security operations to continually monitor the technology resources and analyze the environment for security threats/vulnerabilities and unauthorized access to the Office of Technology network; responds to security requests, problem reports, questions, and incident reports; recommends or takes corrective action and follows-up on corrective actions to ensure that threats and vulnerabilities are addressed.
- Assists in and performs forensic examinations to ensure proper containment and preservation of evidence, tracking of forensic events, maintenance of the chain of custody, and other related tasks.
- Provides assistance with the definition, implementation, maintenance and monitoring of information security requirements for applications, systems and other technology resources.
- Manages and responds to service desk problem tickets to ensure appropriate resolution of issues; analyzes problem tickets to identify issues, patterns, etc. that pose security threats to Office of Technology systems and data.
- Assists in planning and performing audits and assessments of processes, employee practices, network operations and components, servers, telecommunications, applications, and other technology resources for policy and regulatory compliance, threats and vulnerabilities, and weak or missing controls; supports technology tools typically used in audits, assessments, monitoring, analysis, presentations, reporting, and other OISC activities.
- Recommends, drafts, and contributes to the development of information technology and information security policies, procedures, and standards to govern information

technology usage and optimize operations across the Executive Branch; contributes to the communication and enforcement of the West Virginia Office of Technology information security policies, standards, and procedures, as approved by the executive management.

- Maintains and develops information security knowledge and skills by researching technical literature and attending classes, seminars, and conferences.
- Collaborates with and provides security expertise to the West Virginia Privacy Office and State Privacy Officers to assure that privacy concerns are properly addressed; recommends security products, services, and /or procedures to enhance security and deliver operational efficiencies; develops or acquires content for information security courses, articles, bulletins, flyers, Web postings, and other distribution vehicles.
- Contributes to the preparation and presentation of formal information security briefings, seminars, and self-assessment exercises for various parties, such as the Governor's Executive Information Security Team (GEIST), the Security Audit Committee, the Chief Technology Officer, the Chief Information Security Officer, management, Office of Technology Directors, audit clients, and others.
- Makes recommendations and provides consulting services on the development of procurement instruments and the routine procurement of information security products and/or services; reviews, evaluates, and recommends hardware, software, and other information security related procurement requests for consistency with policy and best practices, technical feasibility, potential to enhance operational efficiencies, and the ability to provide secure services.
- Assists in the preparation and presentation of audit and assessment findings, as well as recommendations of options to mitigate risks, achieve policy and regulatory compliance, and strengthen controls.
- Assists in the planning and delivery of policy training and information security awareness training rollout across the Executive Branch; provides support for information security training and awareness activities. Responds to questions and resolves problems related to the on-line Information Security Training Program; coordinates requests for, and develops, customized information security training.
- Monitors employee compliance with information security training policies. Works with OISC training leader, personnel, training units, supervisors, and others to ensure that employees are successfully completing information security awareness and refresher training.
- May represent the Office of Technology OISC with other governmental agencies, other Office of Technology work groups, professional associations, and community organizations.

KNOWLEDGE, SKILLS, AND ABILITIES:

- Knowledge of at least 3 of the 10 recognized information security domains: (1) access controls, (2) application security, (3) business continuity and disaster recovery, (4) cryptography, (5) risk management, (6) regulations, compliance and investigations, (7) operations security, (8) physical security, (9) security architecture, and (10) telecommunications.
- Basic knowledge of information technology software, hardware, terminology, and concepts.

- Basic knowledge of information technology forensic investigations involving the recovery of evidence from computers and other storage media, preservation of evidence, and regulations governing forensic investigations, e-Discovery, etc.
- Ability to develop skills to use tools and technologies to assess, monitor, and document the security state of applications, systems, media, and other technology resources.
- Ability to read, understand, interpret, compile, and apply technical information.
- Ability to communicate effectively, both verbally and in writing.
- Ability to establish and maintain effective working relationships with subordinates, superiors, and the user community.
- Ability to comprehend total web filter operation from limited documentation and apply that knowledge of web filter operation to the agencies web access for their desired web filtering characteristics.
- Deep understanding of computerized equipment utilized in the total environment entailed by the State.
- Ability to reviews and interprets large amounts of data.

MINIMUM QUALIFICATIONS:
Education: Bachelor's Degree from a regionally accredited college or university.
Experience: 4-6 years of full-time or equivalent part-time paid experience in computer science, information security, or other related information technology field.
Education & Experience Substitution: Additional qualifying experience may substitute for the required education on a year-for-year basis.
Certificates, Licenses, Registrations: N/A

CLASS TITLE: Information Security Analyst 2

DISTINGUISHING CHARACTERISTICS:
These positions perform advanced and expert level work in developing, implementing and maintaining information security policies, standards and controls. They serve as subject matter experts for information security related initiatives. They direct audits and assessments to identify and analyze potential threats to data and systems. These positions recommend internal controls and risk management strategies, and assume lead responsibility for the planning, development, implementation and ongoing management of multiple information security programs. These positions have input into setting and are responsible for staying within assigned budgets. They may lead staff when in charge of projects and/or supervise staff within an organizational unit. Perform related work as required.

EXAMPLES OF WORK: ***(Any specific position in this class may not include all of the duties listed; nor do the examples listed cover all of the duties which may be assigned.)***

- Prepares and presents briefings, training, and seminars for/to the Governor's Cabinet, Governor's Executive Information Security Team (GEIST), the Security Audit Committee, the Chief Technology Officer, the Chief Information Security Officer, management, audit clients, and others.

- Leads clients seeking to obtain third-party information security related services, through the development of information security specifications, and the evaluation of vendor responses to ensure that engagement objectives are clearly articulated and the appropriate vendor is selected.
- Oversees third-party Information security engagements to ensure that: third-parties obtain accurate and complete information; engagement objectives are achieved; deliverables comply with contract specifications; costs are controlled by avoiding duplicate or out-of-scope work.
- Manages, assigns, schedules, trains, reviews, evaluates, and oversees the work of subordinates related to functional areas/ strategic initiatives supporting Executive Branch operations.
- Conducts information technology (IT) auditing and information security awareness training to ensure that objectives related to security, internal controls, and technology usage are achieved.
- Conducts periodic risk assessments and develops strategic, long-term audit plans for the Executive Branch to: ensure that security controls operate as expected and in compliance with regulations, policies, and industry standards; identify changes in the technology environment for the purpose of recommending solutions to address those changes. Develops detailed audit programs for specific audit engagements, which include establishing audit objectives, engagement fees, scheduling and reporting requirements, fieldwork templates and questionnaires, work paper management processes, testing and sampling procedures, and reporting requirements.
- Leads and coordinates efforts to deliver an information security awareness training program to the Executive Branch including developing and delivering presentations, designing training materials, and implementing processes to track and report on training results for regulatory compliance purposes.
- Manages the acquisition and employment of external consultants and supplemental staff to support various OISC IT audits, security assessments, and project management activities. This includes the determination of scope, budget and schedule; writing proposals; reviewing and evaluating vendor responses to the proposals; selecting the vendors/consultants to perform work; supervising and monitoring the work to ensure achievement of objectives; and activities associated with closing the engagement.
- Develops / contributes to policies and procedures related to auditing, management, information security training, account management, technology standards, and other information security functions.
- Researches new training topics to address the changing technology environment and security risks associated with those changes.
- Researches technology tools and industry best practices to determine the types of technology needs of the OISC administrative functions; manages the processes to select, implement, operate, and support the technology tools upon deployment.
- Performs administrative duties such as authoring classification specifications and position postings; developing interview questions and criteria for new positions; selecting new employees; developing and delivering presentations for OT staff meetings, committees, and other groups.

- Participates in national and state conferences and meetings to present papers, discuss current industry trends and issues, and share ideas about IT auditing, security, project management and technology acquisitions.

KNOWLEDGE, SKILLS, AND ABILITIES:

- Knowledge of all ten recognized information security domains: (1) access controls, (2) application security, (3) business continuity and disaster recovery, (4) cryptography, (5) risk management, (6) regulations, compliance and investigations, (7) operations security, (8) physical security, (9) security architecture, and (10) telecommunications.
- Knowledge of lifecycle methodologies for data, applications, hardware, and other technology resources.
- Knowledge of information technology architectures, applications, data management, databases and other data repositories, software, hardware, information processing, data center/system operations, networks, and telecommunications.
- Knowledge of programming languages and concepts.
- Knowledge of information technology forensic investigations involving the containment, recovery, and preservation of evidence, as well as, regulations governing forensic investigations, e-Discovery, etc.
- Knowledge of project management principles and practices, such as resource management, tasks and work breakdown structure, schedules, milestones, reporting, and issue tracking.
- Skilled in the use of tools and technologies to assess, monitor, evaluate, document, and report on the security state of applications, systems, media, and other technology resources.
- Ability to analyze and evaluate various work environment and processes to specify security requirements, determine testing criteria, and recommend monitoring techniques.
- Ability to direct and manage diverse teams or groups on projects, of moderate to long duration, that impact numerous operations and processes, and require substantial changes in culture and business practices.
- Ability to make decisions and use independent judgment, especially when resolving complex, challenging issues associated with information security work, projects or operations.
- Ability to read, understand, evaluate, interpret, compile, and apply complex technical information.
- Ability to communicate effectively, both verbally and in writing, to diverse groups, including those serving in management, professional, technical, and staff positions.
- Ability to establish and maintain effective working relationships with subordinates, superiors, and the user community.

MINIMUM QUALIFICATIONS:
Educations: Bachelor's Degree from a regionally accredited college or university in a related information technology field.
Experience: 6-8 years of full-time or equivalent part-time paid experience in computer science.
Education & Experience Substitution: Master's Degree from a regionally accredited college or university may substitute for two (2) years of the required experience.

Certificates, Licenses, Registrations: Must acquire one professional information security certification from a nationally recognized professional organization, or must acquire two technical/specialist information security related certifications.